

## (12)特許協力条約に基づいて公開された国際出願

(19)世界知的所有権機関  
国際事務局(43)国際公開日  
2004年7月1日 (01.07.2004)

PCT

(10)国際公開番号  
WO 2004/055680 A1(51)国際特許分類<sup>7</sup>: G06F 12/14, G06K 19/073

(21)国際出願番号: PCT/JP2003/016000

(22)国際出願日: 2003年12月12日 (12.12.2003)

(25)国際出願の言語: 日本語

(26)国際公開の言語: 日本語

(30)優先権データ:  
特願2002-363597  
2002年12月16日 (16.12.2002) JP

(71)出願人(米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府門真市大字門真1006番地 Osaka (JP).

(72)発明者; および

(75)発明者/出願人(米国についてのみ): 高木 佳彦 (TAKAGI,Yoshihiko) [JP/JP]; 〒144-0046 東京都大田区東六郷2-20-5-506 Tokyo (JP). 中西 良明 (NAKANISHI,Yoshiaki) [JP/JP]; 〒166-0014 東京都杉並区松ノ木2-4-10-305 Tokyo (JP). 佐々木理 (SASAKI,Osamu) [JP/JP]; 〒144-0046 東京都大田区東六郷2-20-5-620 Tokyo (JP). 菊地 隆文 (KIKUCHI,Takafumi) [JP/JP]; 〒144-0046 東京都大田区東六郷2-20-5-718 Tokyo (JP).

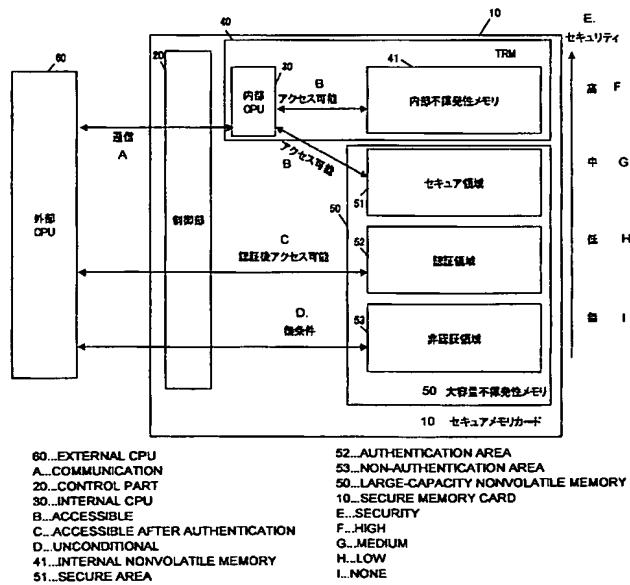
(74)代理人: 小栗 昌平, 外(OGURI,Shohei et al.); 〒107-6013 東京都港区赤坂一丁目12番32号アーク森ビル13階 栄光特許事務所 Tokyo (JP).

(81)指定国(国内): CN, KR, US.

(締葉有)

(54)Title: MEMORY DEVICE AND ELECTRONIC DEVICE USING THE SAME

(54)発明の名称: メモリデバイスとそれを使用する電子機器



(57)Abstract: A memory card having a large storage capacity and a memory area that has an equivalent level of security to IC cards. A semiconductor memory card (10) attachable to and removable from an electronic device has a non-tamper-resistant first memory (50) comprising ordinary areas (52,53) that are accessible from the electronic device and a secure area (51) that is not directly accessible from the electronic device, and also has a tamper-resistant second memory (41) that is not directly accessible from the electronic device. The semiconductor memory card (10) is so configured that the secure area (51) of the first memory (50) can be accessed only via a secure control part (30) that manages the access to the second memory (41). The secure area (51) cannot be directly accessed from any external device and hence exhibits a higher security level than an authentication area (52). Moreover, since the secure area (51) is provided in the non-tamper-resistant memory (50), it can have a large storage capacity.

(締葉有)

WO 2004/055680 A1



(84) 指定国(広域): ヨーロッパ特許(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 國際調査報告書

---

(57) 要約: 本発明は、記憶容量が大きく、且つ、ICカードと同等のセキュリティレベルを有するメモリ領域を備えたメモリカードを提供することを目的とする。電子機器に着脱可能な半導体メモリカード10に、電子機器からアクセスすることが可能な通常領域52,53と、電子機器から直接アクセスすることができないセキュア領域51とを有する非耐タンパー性の第1のメモリ50と、電子機器から直接アクセスすることができない耐タンパー性の第2のメモリ41とを設け、第1のメモリ50のセキュア領域51へのアクセスが、第2のメモリ41へのアクセスを管理するセキュア制御部30を介してのみ可能であるように構成している。このセキュア領域51は、外部機器が直接アクセスできないため、認証領域52よりもセキュリティレベルが高い。また、このセキュア領域51は、非耐タンパー性のメモリ50に設けられるため、記憶容量を大きく取ることができる。

## 明細書

## メモリデバイスとそれを使用する電子機器

## 5 &lt;技術分野&gt;

本発明は、半導体メモリカードなどのメモリデバイスと、このメモリデバイスへのデータの書き込み／読み出しを行う電子機器に関し、特に、セキュリティレベルが高く、大きい記憶容量を持つ記憶媒体の実現を図るものである。

## 10 &lt;背景技術&gt;

不揮発性の半導体メモリを記憶媒体として具備する半導体メモリカード（以下、「メモリカード」と言う）は、DVDなどのディスク状記憶媒体に比べて、記憶容量は小さいが、大きな機構部を必要とせず、小型で取り扱いが容易で、耐震性にも優れているため、携帯用に好適な記憶媒体として、最近、その利用範囲が拡大している。

メモリカードには、CPU（マイコン）を内蔵したものとCPUを内蔵しないものとがある。CPUを内蔵したメモリカードにおけるCPUの働きは、外部機器から要求される、不揮発性メモリの読み出し・書き込み処理である。

また、メモリカードの不揮発性メモリにセキュア領域を設けて、セキュリティレベルを高める工夫も行われている。下記特許文献1には、不揮発性メモリ内に、認証に成功した外部機器のみがアクセスできる認証領域と、外部機器のいずれもがアクセスできる非認証領域とを設けたメモリカードが記載されている。このメモリカードを用いて、暗号化した音楽コンテンツを非認証領域に格納し、それを復号する復号鍵を認証領域に格納することにより、コンテンツの著作権を守ることが可能になる。

このようなメモリカードにおけるCPUの働きは、読み出し・書き込み処理に加えて、外部機器による認証領域へのアクセスを許可するための外部機器の認証処理がある。

いずれにしろ、メモリカードにおけるCPUの働きは、メモリの読み書き及びそれに付随したものに限定され、メモリに記録されたデータの制御は外部機器によって行われる。

一方、同様にCPUを内蔵するICカードは、耐タンパー性のモジュール内に5 CPUとともにメモリ領域を有している。耐タンパーゆえ、外部機器は、このメモリ領域に直接アクセスすることができない。そのため、ICカードは、複製や偽造に対して高い守秘性があり、高いセキュリティレベルが要求されるデジタルキャッシュのサービス等で利用されている。

ICカードにおけるCPUの働きは、メモリの読み出し・書き込みのみならず、10 外部から入力されたデータの暗号化、署名生成、署名検証、入力された暗証番号照合など、多岐に渡る。また、ICカードのメモリに記録されたデータの制御はICカード内部CPUによって行われる。

このように、ICカードのCPUは、従来のメモリカードに内蔵されるCPUに比べて、多機能かつ高セキュリティである。

15

#### [特許文献1]

特開2001-14441号公報

しかし、ICカードは、蓄積できる情報容量が限られており、デジタルキャッシュのサービスの多様化と共に、蓄積容量の拡大がサービス業者等から求められている。例えば、デジタルキャッシュの2重引き落とし等のトラブルを回避する目的で、電子レシートや取引ログを記録するサービスを実施しようとすると、累積する電子レシート等を蓄積するために、従来のICカードの容量に比べて、大きな情報容量の確保が必要になる。

一方、前記特許文献1に記載されているメモリカードは、認証領域が可変に設定できるため、ある程度大きな情報容量を持たせることが可能である。しかし、この認証領域は、外部機器が直接制御可能な領域であるため、ICカードに比べてセキュリティレベルは低い。

## &lt;発明の開示&gt;

本発明は、こうした従来の問題点を解決するものであり、記憶容量が大きく、且つ、ICカードと同等のセキュリティレベルを有するメモリ領域を備えたメモリデバイスを提供し、また、そのメモリデバイスを使用する電子機器を提供する  
5 ことを目的としている。

そこで、本発明では、電子機器に固定的にまたは着脱可能に接続されるメモリデバイスに、電子機器からアクセスすることが可能な通常領域と、電子機器から直接アクセスすることができないセキュア領域とを有する非耐タンパー性の第1のメモリと、電子機器から直接アクセスすることができない耐タンパー性の第2のメモリとを設け、第1のメモリのセキュア領域へのアクセスが、第2のメモリへのアクセスを管理するセキュア制御部を介してのみ可能であるように構成している。  
10

このセキュア領域は、外部機器が直接アクセスできないため、従来の認証領域よりもセキュリティレベルが高い。また、このセキュア領域は、非耐タンパー性  
15 のメモリに設けているため、低コストで大きい記憶容量を取ることができる。

また、本発明では、メモリ領域として第1領域、第2領域及び第3領域を有するメモリデバイスに対してアクセスを行う電子機器が、メモリデバイスへのアクセス要求を受けたときに、メモリデバイスの非耐タンパー性のメモリ領域である第1領域には、メモリデバイスへのアクセスを制御するメモリデバイスの全体制御部を介してアクセスを行い、第1領域以外の非耐タンパー性のメモリ領域である第2領域には、全体制御部と、第2領域及び第3領域へのアクセスを制御するメモリデバイスのセキュア制御部とを介して、セキュア制御部との認証を経た後、アクセスを行い、また、メモリデバイスの耐タンパー性のメモリ領域である第3領域には、全体制御部及びセキュア制御部を介して、セキュア制御部との認証を  
20 経た後、アクセスを行うように構成している。  
25

この電子機器は、この半導体メモリカード等のメモリデバイスを活用して、多様なサービスの実現を図ることができる。

## &lt;図面の簡単な説明&gt;

図1は、本発明の実施形態におけるセキュアメモリカードの概念図；

図2は、本発明の実施形態におけるセキュアメモリカードの構成を示すブロック図；

図3は、本発明の実施形態におけるセキュアメモリカードを使用するシステムの概念図；

図4は、本発明の実施形態におけるR/W装置の構成を示すブロック図；

図5は、本発明の実施形態におけるセキュアメモリカードの書き込み手順を示すシーケンス；

図6は、本発明の実施形態におけるセキュアメモリカードの書き込み手順の続きを示すシーケンス；

図7は、本発明の実施形態におけるセキュアメモリカードの他の書き込み手順を示すシーケンス；

図8は、本発明の実施形態におけるセキュアメモリカードの大容量不揮発性メモリの構造を示す図；

図9は、本発明の実施形態における論理一物理アドレス変換テーブルを示す図；

図10は、本発明の実施形態における論理一物理アドレス変換テーブルの他の例を示す図；

図11は、本発明の実施形態におけるセキュアメモリカードの大容量不揮発性メモリの異なる構造を示す図；

図12は、本発明の実施形態における論理一物理アドレス変換テーブルの異なる例を示す図である。

尚、図中の参照番号は、10—セキュアメモリカード；11—I C部；12—I/F部；13—I Cコマンド処理部；14—ファイル管理部；15—I C認証部；16—メモリ管理部；17—暗復号回路；18—内部不揮発性メモリI/F部；20—制御部；21—データI/F部；22—コマンドI/F部；23—制御認証部；24—コマンド処理部；25—アクセス制御部；26—大容量不揮発性メモリI/F部；40—TRM；41—内部不揮発性メモリ；50—

大容量不揮発性メモリ；5 1——セキュア領域；5 2——認証領域；5 3——非認証領域；6 0——外部C P U；6 1——携帯電話；6 2——R O M；6 3——R A M；6 4——液晶表示部；6 5——無線通信部；6 6——操作ボタン；6 7——カードI／F部；6 8——認証回路；6 9——R／W装置；7 0——内部バス；9 1——チャージ用端末；9 5——チャージサーバ；9 3——決済サーバ；9 4——配信サーバ；9 5——ネットワーク；6 2 1——コマンド生成プログラム；6 2 2——認証鍵群  
5 を示すものである。

＜発明を実施するための最良の形態＞

10 本発明の実施形態における半導体メモリカード（ここでは「セキュアメモリカード」と呼ぶことにする）は、図1の概念図に示すように、内部不揮発性メモリ4 1を備える耐タンパー性モジュール（tamper resistant module: T R M）4 0と、非認証領域5 3、認証領域5 2及びセキュア領域5 1を備える大容量不揮発性メモリ5 0と、内部不揮発性メモリ4 1及びセキュア領域5 1に対してアクセスする内部C P U3 0と、電子機器（リード／ライト（R／W）装置）の外部C P U6 0と通信して認証処理を行い、認証した外部C P U6 0の認証領域5 2へのアクセスを許可する制御部2 0とを備えている。

20 T R M4 0の不揮発性メモリ4 1は、例えば、1 6バイト単位で消去・書き込みができるE E P R O Mから成り、また、大容量不揮発性メモリ5 0は、例えば、5 1 2バイト等のブロック単位での消去と1バイト単位での書き込みとが可能なフラッシュメモリから成る。

25 外部C P U6 0は、非認証領域5 3に無条件でアクセスすることができ、また、認証領域5 2には、制御部2 0での認証を済ませた場合にアクセスすることができる。しかし、外部C P U6 0は、セキュア領域5 1及び内部不揮発性メモリ4 1の存在を知ることができず、これらに直接アクセスすることはできない。

セキュア領域5 1及び内部不揮発性メモリ4 1に対しては、内部C P U3 0だけがアクセス可能である。セキュア領域5 1と内部不揮発性メモリ4 1との違いは、内部不揮発性メモリ4 1がT R M4 0に設けられているのに対し、セキュア領域5 1が、耐タンパー性を持たない大容量不揮発性メモリ5 3に設けられて

る点である。そのため、セキュア領域 5 1 は、内部不揮発性メモリ 4 1 に比べて大きい蓄積容量を持つことができる。その反面、セキュリティレベルは、TRM 4 0 に設けられた内部不揮発性メモリ 4 1 よりも低い。この 4 つの領域のセキュリティレベルは、非認証領域 5 3 が最も低く、認証領域 5 2 、セキュア領域 5 1 、  
5 内部不揮発性メモリ 4 1 の順に高くなっている。

セキュアメモリカード 1 0 の構成の詳細は後述するとして、その使用形態について説明する。

セキュアメモリカードは、例えば、図 3 に示す音楽配信システムなどで使用することができる。このシステムでは、セキュアメモリカード 1 0 が R/W 装置である携帯電話 6 1 に装着される。また、このシステムには、ネットワーク 9 5 を介して音楽を配信する配信サーバ 9 4 と、決済処理を行う決済サーバ 9 3 と、デジタルキャッシュをメモリカード 1 0 にチャージするチャージサーバ 9 2 と、デジタルキャッシュのチャージ用端末 9 1 とが存在している。

携帯電話 6 1 は、図 4 のブロック図に示すように、図 1 の外部 CPU に相当する CPU 6 0 と、認証に使用する認証鍵群 6 2 2 やコマンド生成プログラム 6 2 1 を予め記憶している ROM 6 2 と、CPU 6 0 の作業領域として使用される RAM 6 3 と、表示画面を構成する液晶表示部 6 4 と、ネットワークを介して無線通信を行う無線通信部 6 5 と、ユーザが操作する操作ボタン 6 6 と、セキュアメモリカード 1 0 を内部バス 7 0 に接続するカード I/F 部 6 7 と、セキュアメモリカード 1 0 との相互認証を行う認証回路 6 8 とを備えており、これらの各部が内部バス 7 0 で接続されている。

ユーザは、まず、セキュアメモリカード 1 0 にデジタルキャッシュをチャージする。そのために、ユーザは、セキュアメモリカード 1 0 をチャージ端末 9 1 に装着し、表示された指示に従ってチャージ端末 9 1 を操作する。このとき、チャージ端末 9 1 は、セキュアメモリカード 1 0 の内部 CPU 3 0 に入金アプリケーションの起動を要求する。入金アプリケーションを起動した内部 CPU 3 0 は、チャージ端末 9 1 からデジタルキャッシュの入金処理要求を受けると、その要求のコマンドから、データの書き込み先を内部不揮発性メモリ 4 1 と判断し、チャ

ージ端末 9 1 から伝えられた金額を内部不揮発性メモリ 4 1 に書き込む。こうして内部不揮発性メモリ 4 1 にキャッシュ情報が蓄積される。

また、デジタルキャッシュのチャージは、セキュアメモリカード 1 0 を装着した携帯電話 6 1 から、チャージサーバ 9 2 にアクセスして、オンラインで行うこ  
5 ともできる。

次に、ユーザは、携帯電話 6 1 から配信サーバ 9 4 にアクセスし、音楽コンテンツの購入を依頼する。配信サーバ 9 4 は、音楽コンテンツの代金の決済を要求する。これを受けた携帯電話 6 1 の CPU 6 0 は、セキュアメモリカード 1 0 の内部 CPU 3 0 に決済アプリケーションの起動を要求する。決済アプリケーションを起動した内部 CPU 3 0 は、携帯電話 6 1 を認証した後、携帯電話 6 1 から伝えられた支払額を内部不揮発性メモリ 4 1 に記録されたデジタルキャッシュの残額から減算する。これを受けた配信サーバ 9 4 は、電子レシートを携帯端末 6 1 に送信し、携帯端末 6 1 の CPU 6 0 は、この電子レシートの格納要求をセキュアメモリカード 1 0 の内部 CPU 3 0 に送る。内部 CPU 3 0 は、その要求の  
10  
15 コマンドから、データの書き込み先をセキュア領域 5 1 と判断して、電子レシートをセキュア領域 5 1 に蓄積する。

なお、決済処理は、内部不揮発性メモリ 4 1 に格納されたクレジット番号を決済サーバ 9 3 に提示して、決済サーバ 9 3 との間で行うこともできる。

決済の終了後、配信サーバ 9 4 は、暗号化された音楽コンテンツと、その復号  
20 鍵とを携帯電話 6 1 に送信する。携帯電話 6 1 の CPU 6 0 は、受信データを判  
断し、コンテンツの復号鍵をセキュアメモリカード 1 0 の認証領域 5 2 に格納し、  
また、暗号化されたコンテンツをセキュアメモリカード 1 0 の非認証領域 5 3 に  
格納する。

このように、このシステムでは、セキュアメモリカード 1 0 の TRM 4 0 の内  
25 部不揮発性メモリ 4 1 にはキャッシュ情報が格納され、セキュア領域 5 1 には電  
子レシートが、認証領域 5 2 には復号鍵が、また、非認証領域 5 3 には暗号化さ  
れたコンテンツがそれぞれ格納される。

図 2 のブロック図は、セキュアメモリカード 1 0 の構成を示している。セキュアメモリカード 1 0 は、大別して、制御部 2 0 と、大容量不揮発性メモリ 5 0 と、

図1のTRM40に相当するIC部11とで構成される。大容量不揮発性メモリ50は、非認証領域53と、認証領域52と、セキュア領域51と、これらの領域のアドレス情報が格納されたアドレス情報管理領域54とを有している。

制御部20は、R/W装置69との間でデータの授受を行うデータI/F部21と、R/W装置69との間でコマンドの授受を行うコマンドI/F部22と、R/W装置69を認証する制御認証部23と、受け付けたコマンドを解釈してコマンドに応じた処理を行う制御コマンド処理部24と、大容量不揮発性メモリ50へのアクセスを制御するとともにIC部11とのデータの受け渡し窓口となるアクセス制御部25と、大容量不揮発性メモリ50との間でデータを受け渡す大容量不揮発性メモリI/F部26とを備えている。

また、耐タンパ一性のIC部11は、内部不揮発性メモリ41と、制御部20との間でデータやコマンドの授受を行うI/F部12と、コマンドを解釈してコマンドに応じた処理を行うICコマンド処理部13と、内部不揮発性メモリ41及びセキュア領域51にファイル形式で格納されたデータを管理するファイル管理部14と、R/W装置69を認証し、認証したR/W装置69に対して内部不揮発性メモリ41及びセキュア領域51へのデータアクセスを許可するIC認証部15と、内部不揮発性メモリ41及びセキュア領域51への書き込み/読み出しデータに対して内部不揮発性メモリ41に格納された鍵を用いて暗号化/復号化を行う暗復号回路17と、内部不揮発性メモリ41及びセキュア領域51の管理を行うメモリ管理部16と、内部不揮発性メモリ41へのデータの授受を行う内部不揮発性メモリI/F部18とを備えている。特許請求の範囲で云うセキュア制御部は、IC部11のICコマンド処理部13、IC認証部15、暗復号回路17、ファイル管理部14及びメモリ管理部16に対応する。

制御部20の制御コマンド処理部24は、R/W装置69から受信したコマンドを解釈し、そのコマンドが

- ・大容量不揮発性メモリ50の認証領域52または非認証領域53へのアクセスを要求するものであるか、
- ・認証を要求するものであるか、
- ・IC部11による処理を要求するものであるか

を判断し、大容量不揮発性メモリ 50 の認証領域 52 または非認証領域 53 へのアクセスを要求しているときは、アクセス制御部 25 に大容量不揮発性メモリ 50 へのアクセス制御を指示し、IC 部 11 による処理を要求しているときは、アクセス制御部 25 に IC 部 11 へのコマンドの転送を指示し、また、認証を要求 5 しているときは、制御認証部 23 に認証処理を指示する。

認証領域 52 へのアクセスは、その端末に対する制御認証部 23 の認証が済んでいる場合にのみ、受け入れられる。

アクセス制御部 25 は、大容量不揮発性メモリ 50 へのアクセス制御に当たって、大容量不揮発性メモリ 50 のアドレス情報管理領域 54 に記録されたアドレス情報を参照する。端末 (R/W 装置 69) が大容量不揮発性メモリ 50 の論理アドレスを指定してアクセスを求めて来たときは、アドレス情報管理領域 54 の記録から、指定されたアドレスが大容量不揮発性メモリ 50 のいずれの領域に属 10 しているかを判断し、認証領域 52 へのアクセス要求に対しては、認証済み端末に限って許可する。

また、IC 部 11 の IC コマンド処理部 13 は、制御部 20 から送信されたコ 15 マンドを解釈し、その処理要求が、

- ・内部不揮発性メモリ 41 へのデータ書き込み／読み出しを要求するものであるか、
- ・セキュア領域 51 へのデータ書き込み／読み出しを要求するものであるか、
- ・認証を要求するものであるか、
- ・その他の処理を要求するものであるか

を判断する。

IC コマンド処理部 13 は、コマンドがアプリケーションの起動を要求しているときには、内部にそのアプリケーションを起動する。

アプリケーションとは、R/W 装置 69 から受け取ったコマンドの解釈形態で 25 あり、アプリケーション起動後に R/W 装置 69 から IC コマンド処理部 13 が受け取ったコマンドは、そのアプリケーションと R/W 装置 69 との間で取り決めた解釈が IC コマンド処理部 13 によって行われる。

アプリケーション起動後に受け取ったコマンドが、認証を要求しているときには、ICコマンド処理部13は、IC認証部15にR/W装置69の認証処理を指示する。

また、ICコマンド処理部13は、コマンドが、内部に起動したアプリケーションとR/W装置69との間で取り決めた、内部不揮発性メモリ41へのデータの書き込み/読み出し、または、セキュア領域51へのデータの書き込み/読み出しを要求するコマンドであるときは、IC認証部15において認証処理が済まされているか確認する。

認証処理が済まされている場合は、その要求を許可し、その要求が書き込み求めるときは、書き込むデータを、格納先の情報を付してメモリ管理部16に送る。

内部不揮発性メモリ41及びセキュア領域51を管理するメモリ管理部16は、書き込むデータを暗復号回路17で暗号化（このとき暗復号回路17は、内部不揮発性メモリ41に格納された暗号鍵を用いて暗号化を行う）した後、内部不揮発性メモリ41に書き込むべきデータを、内部不揮発性メモリI/F部18を介して、内部不揮発性メモリ41に書き込み、書き込み位置の情報をファイル管理部14に伝える。また、セキュア領域51に書き込むべきデータを、大容量不揮発性メモリI/F部26を介して、大容量不揮発性メモリ50のセキュア領域51に書き込み、書き込み位置の情報をファイル管理部14に伝える。

ファイル管理部14は、メモリ管理部16から伝えられた情報を基に、内部不揮発性メモリ41及びセキュア領域51に格納されたファイルを管理する。

また、ICコマンド処理部13は、その要求が読み出し要求であるときは、読み出すべきデータのファイル位置をファイル管理部14に求め、メモリ管理部16にそのファイルの読み出しを要求する。

メモリ管理部16は、そのファイルをメモリ管理部16が内部不揮発性メモリ41またはセキュア領域51から読み出すと、暗復号回路17でデータを復号化（このとき暗復号回路17は、内部不揮発性メモリ41に格納された鍵を用いて復号化を行う）して、ICコマンド処理部13に送る。

復号化されたデータは、制御部20に送られ、データI/F部21からR/W装置69に送信される。

ここで、大容量不揮発性メモリ50の非認証領域53、認証領域52及びセキュア領域51、並びに内部不揮発性メモリ41への書き込み／読み出し条件を整5理すると次のようになる。

- ・非認証領域：無条件でアクセス可能である。非認証領域53にアクセスするための通常コマンドでデータの書き込み／読み出しを行うことができる。
- ・認証領域：制御部20の制御認証部23との認証を済ませることが必要である。

制御認証部23が認証することによって認証領域52の論理アドレスを用いてア10クセスすることが可能となる。

・セキュア領域：IC部11のIC認証部15（＝IC部アプリケーション）との認証を済ませることが必要である。IC部アプリケーションと端末との間で取り決めたコマンドによりデータの書き込み／読み出しが可能になる（またはIC部アプリケーションの処理の一部としてデータの書き込み／読み出しが可能になる）。端末からはセキュア領域を見ることができず、端末は、セキュア領域の論15理アドレスを用いてアクセスすることはできない。

- ・内部不揮発性メモリ：セキュア領域の書き込み／読み出し条件と全く同じである。なお、セキュア領域にアクセスするための認証と内部不揮発性メモリにアクセスするための認証とを異なるものとしてもよい。

20 図8は、大容量不揮発性メモリ50の内部構造を示している。ここでは、大容量不揮発性メモリ50の物理アドレス上の配置が、非認証領域53は0000～(XXXX-1)、認証領域52はXXXX～(ZZZZ-1)、セキュア領域51はZZZZ～(YYYY)の場合を示している。セキュア領域51と認証領域52との境界を示す第1アドレス情報はZZZZであり、認証領域52と非認証領域53との境界を示す第2ア25ドレス情報はXXXXである。また、非認証領域53のサイズはXXXX、認証領域52のサイズはZZZZ-XXXX、セキュア領域51のサイズはYYYY-ZZZZ+1である。

図9は、各領域の物理アドレスと論理アドレスとの対応関係を表す「論理-物理アドレス変換テーブル」を示している。非認証領域53の論理アドレスは

0000～(XXXX-1)であり、認証領域52の論理アドレスは0000～(ZZZZ-XXXX-1)、セキュア領域51の論理アドレスは0000～(YYYY-ZZZZ)である。

アドレス情報管理領域54には、第1アドレス情報、第2アドレス情報、及び、各領域の論理-物理アドレス変換テーブルが保持されている。非認証領域53、  
5 認証領域52、及びセキュア領域51のいずれについても、割り当てられた論理アドレスの境界を越えて論理アドレスを指定することはできないが、各領域の境界を移動して、各領域を拡張または縮小することはできる。

セキュア領域51の拡張/縮小は、第1アドレス情報を変更することによって実現できる。図9の論理-物理アドレス変換テーブルでは、非認証領域53及び  
10 認証領域52における論理アドレスの順番を物理アドレスの順序の正順とし、セキュア領域51における論理アドレスの順番を物理アドレスの順序の逆順としているので、認証領域52とセキュア領域51との境界を変更したとき、ともに論理ブロックの末尾アドレスの側だけを修正すれば足りるので、境界変更に伴うテーブルの書き換え負担が少なくなり、高速での処理が可能になる。

15 この境界変更の手順については後述する。

次に、このセキュアメモリカードでのデータの格納手順について説明する。

図5及び図6は、セキュアメモリカードを装着した端末から配信サーバにコンテンツ購入を依頼し、代金の決済処理を行い、その電子レシートをセキュア領域に、暗号化されたコンテンツを非認証領域に、また、コンテンツの復号鍵を認証  
20 領域に格納するまでの手順を示している。

図5に示すように、端末は配信サーバにコンテンツ購入を依頼する(1)。配信サーバは、コンテンツの代金の決済を要求する(2)。端末は、セキュアメモリカード10のIC部11に決済アプリケーションの起動を要求するコマンドを送信する(3)。制御部20の制御コマンド処理部24は、このコマンドをIC部  
25 部に対するコマンドであると認識して、IC部11に送信する(4)。IC部11は、決済アプリケーションを起動してIC認証部15を立ち上げ、応答を端末に返す(5)、(6)。端末は、セキュアメモリカード10に認証要求コマンドを送り(7)、制御部20の制御コマンド処理部24は、このコマンドをIC部に対するコマンドであると認識して、IC部11に送信する(8)。IC認証部

15は、端末（または配信サーバ）を認証し、認証結果を応答する（9）、（10）。認証が済んだ端末は、セキュアメモリカード10に支払額を示し、決済要求のコマンドを送信する（11）。制御部20の制御コマンド処理部24は、このコマンドをIC部に対するコマンドであると認識して、IC部11に送信する  
5（12）。IC認証部15は、「決済要求」というコマンドにより内部不揮発性メモリ41に書き込むデータであることを判断し、内部不揮発性メモリ41に記録された残高を、支払額を減算した額に書き換える処理を行い、処理終了を応答する（13）、（14）（なお、端末が（9）の認証を済ませていない状態での決済要求は拒否される）。

10 端末は、配信サーバに応答を返す（15）。配信サーバは電子レシートを端末に送信する（16）。端末は、セキュアメモリカード10に電子レシートの格納要求コマンドを送信する（17）。制御部20の制御コマンド処理部24は、このコマンドをIC部に対するコマンドであると認識して、IC部11に送信する。  
15 IC認証部15は、「電子レシート格納要求」というコマンドによりセキュア領域51に格納すべきデータであると判断し、電子レシートを暗復号回路17で暗号化した後、セキュア領域51に格納する（18）（なお、端末が（9）の認証を済ませていない状態での電子レシート格納要求は拒否される）。

なお、IC認証部15による（9）の認証は、「決済要求」を許可するための認証と、「電子レシート格納要求」を許可するための認証とを別に行うようにしてもよい（つまり、異なる鍵を用いて認証することを必要とする、としてもよい）。

図6に示すように、電子レシートの格納済みの応答がIC部11から端末に送られると（19）（20）、端末は配信サーバにコンテンツの送信を要求する（21）。配信サーバは、暗号化したコンテンツと、それを復号するコンテンツ鍵とを端末に送信する（22）。端末は、配信サーバから受け取ったデータに、認証領域52に書き込むべきコンテンツ鍵が含まれることを判断し、セキュアメモリカード10の制御部20に対して認証を要求する（23）。制御部20の制御コマンド処理部24は、このコマンドを解釈して、端末の認証を制御認証部23で行わせて、認証結果を応答する（24）。端末は、認証領域52へのコンテ

ンツ鍵の書き込み要求を出す（25）。制御部20のアクセス制御部25は、端末の認証が済んでいるため、認証領域52へのアクセスを許可し、認証領域52にコンテンツ鍵が書き込まれる。書き込み終了の応答があると（26）、端末は、暗号化されたコンテンツを非認証領域53へ書き込むべきことを判断し、セキュアメモリカード10に非認証領域53へのコンテンツの書き込みを要求する（27）。暗号化されたコンテンツが非認証領域53に書き込まれ、その応答が端末に返ると（28）、端末は配信サーバに完了通知を送信する（29）。

こうして、電子レシートが暗号化してセキュア領域51に、コンテンツ鍵が認証領域52に、暗号化されたコンテンツが非認証領域53に、それぞれ書き込まれる。

なお、図5の手順中、内部不揮発性メモリ41に記録された残高を、支払額を減算した額に書き換えたとき（13）、図7に示すように、その支払額をセキュア領域51に書き込むようにしても良い（13'）。こうすることで決済ログをセキュア領域51に記録することができる。

また、決済アプリケーションによる認証（3）を行う前、または後に、利用者を確認するための暗証番号照合を行うようにしてもよい。

次に、大容量不揮発性メモリ50における各領域間の境界変更の手順について説明する。ここでは、図8の第1アドレス情報を変更してセキュア領域51を拡張または縮小する場合を示す。

この境界変更は、セキュアメモリカード10を装着した端末からの要求で行われる。

（1）端末は、セキュアメモリカード10に対して、境界変更アプリケーションの起動を要求し、このアプリケーションを起動したセキュアメモリカード10のIC部11は、ICコマンド処理部13及びIC認証部15を立ち上げる。端末は、IC部11に対して認証を要求し、IC認証部15は、端末を認証する。なお、この認証は、内部不揮発性メモリ41やセキュア領域51へのアクセスに要する認証とは別の認証とし、一部の特定端末のみがセキュア領域51の拡張／縮小を行うことができるようにも良い。

(2) 認証を受けた端末は、IC部アプリケーション（ICコマンド処理部13）に対して変更後の第1アドレス情報（新たなZZZZ）を通知する。

(3) ICコマンド処理部13は、メモリ管理部16に新たなZZZZを伝えてセキュア領域51の境界変更を指示する。メモリ管理部16は、ZZZZの値に対応するようにセキュア領域51と認証領域52との論理-物理アドレス変換テーブルを修正し、アドレス情報管理領域54に、新たなZZZZの値と、修正した論理-物理アドレス変換テーブルとを格納する。このとき、図9のセキュア領域及び認証領域のテーブル上で、共に論理ブロックの末尾アドレスの側だけが修正される。

10 (4) メモリ管理部16は、セキュア領域51を拡張した場合には、新たにセキュア領域となった部分のデータを消去し、セキュア領域51を縮小した場合には、新たに認証領域52となった部分のデータを消去する。このとき、セキュア領域、及び／または、認証領域のすべてのデータを消去してもよい。

(5) ICコマンド処理部13は、端末に境界変更完了を通知する。

15 また、このとき、IC部の要求に基づいて、セキュアメモリカード10の制御部20が、境界変更の処理を行うようにしてよい。この場合の手順は次のようになる。

(1) 前記(1)と同様に、端末がIC認証部15の認証を受ける。

20 (1') 端末は、セキュアメモリカード10の制御部20に対して認証を要求し、制御コマンド処理部24の指示により、制御認証部23が認証領域のサイズ変更を許可するための認証を行う。

(2) 前記(2)と同様に、端末が、ICコマンド処理部13に対して変更後の第1アドレス情報（新たなZZZZ）を通知する。

25 (3) ICコマンド処理部13は、アクセス制御部25を経由して、制御部コマンド処理部24に境界アドレス変更を要求する。

(3') 制御部コマンド処理部24は、アドレス情報管理領域54にZZZZの値を保存し、あわせて、ZZZZの値に対応するようにセキュア領域と認証領域との論理-物理アドレス変換テーブルを修正する。（ただし、(1')の認証が行われ

ていない場合は境界アドレスの変更を拒否し、拒否したことを I C コマンド処理部 13 に通知する)

(4) 制御部コマンド処理部 24 は、セキュア領域を拡張した場合に、新たにセキュア領域となった部分のデータを消去し、セキュア領域を縮小した場合に、新たに認証領域となった部分のデータを消去する。また、セキュア領域、及び／または、認証領域のすべてのデータを消去してもよい。

(5) 制御部コマンド処理部 24 は、I C コマンド処理部 13 に境界変更完了を伝え、I C コマンド処理部 13 は、端末に境界変更完了を通知する（ただし、

10 (3') において境界アドレスの変更が拒否された場合は、端末に境界変更の拒否を通知する）。

また、認証領域の拡張／縮小は、認証領域と非認証領域との境界の第 2 アドレス情報を変更することにより行う。この場合の手順は次のようになる。

(1) 端末は、セキュアメモリカード 10 の制御部 20 に対して認証を要求し、制御コマンド処理部 24 の指示により、制御認証部 23 が認証領域のサイズ変更 15 を許可するための認証を行う。

(2) 認証を受けた端末は、制御部 20 に対して変更後の第 2 アドレス情報（新たな XXXX）を通知する。

(3) 制御部コマンド処理部 24 は、アドレス情報管理領域 54 に XXXX の値を保存し、あわせて、XXXX の値に対応するように非認証領域と認証領域との論理 20 一物理アドレス変換テーブルを修正する（ただし、(1) の認証が行われていない場合は境界アドレスの変更を拒否し、拒否したことを端末に通知する）。

(4) 制御部コマンド処理部 24 は、認証領域を拡張した場合に、新たに認証領域となった部分のデータを消去し、認証領域を縮小した場合に、新たに非認証領域となった部分のデータを消去する。また、非認証領域、及び／または、認証 25 領域のすべてのデータを消去してもよい。

(5) 制御部コマンド処理部 24 は、端末に境界変更完了を通知する。

なお、この場合、図 10 に示すように、論理一物理アドレス変換テーブルの非認証領域 53 における論理アドレスの順番が物理アドレスの順序の正順であり、認証領域 52 における論理アドレスの順番が物理アドレスの順序の逆順であると、

境界変更の際に、ともに論理ブロックの末尾アドレスの側だけを修正すれば足りるので、境界変更に伴うテーブルの書き換え負担が少なくなり、高速での処理が可能になる。

非認証領域の拡張／縮小は、認証領域の拡張／縮小処理により実現できる。

5 また、大容量不揮発性メモリ 50 には、図 11 に示すように、セキュア領域 5  
1、非認証領域 53、認証領域 52 の順に各領域を配置しても良い。図 12 には、  
このときの論理一物理アドレス変換テーブルの一例を示している。

10 また、この場合、セキュア領域 51 を端末から見えない領域とするため、または、  
セキュア領域を持たないメモリカードとの互換性を保つために、図 11 に示すように、  
実際の境界アドレスとは異なる「端末みなしアドレス」を設けるようにしてもよい。  
この端末みなしアドレスでは、セキュア領域を省いて、非認証領域 53 の先頭のみなし物理アドレスを 0000 とし（実際は XXXX'）、非認証領域 53 と認証領域 52 との境界のみなし物理アドレスを ZZZZ'（実際は ZZZZ'）、認証領域終端のみなし物理アドレスを YYYY'（実際は YYYY'）とする。端末は境界ア  
15 ドレスを ZZZZ' と認識し、領域の拡張／縮小を要求する際に、この ZZZZ' の変更を要求するが、制御コマンド処理部は、ZZZZ' と ZZZZ' との関係を認識し、実際の物理アドレス ZZZZ' に置き換えて、境界の変更を行う。

20 なお、本発明の実施形態では、大容量不揮発性メモリ 50 に、記憶領域として、  
非認証領域、認証領域及びセキュア領域の 3 領域を設ける場合について説明した  
が、大容量不揮発性メモリ 50 に、セキュア領域の他に、非認証領域または認証  
領域の一方だけを通常領域として設けるようにしても良い。

25 また、ここでは主に、セキュアメモリカードの I C 部に決済用アプリケーションを搭載する場合について説明したが、その他、署名を生成するアプリケーションを搭載することも可能である。

この場合、データのセキュア領域への書き込み時に書き込みデータのハッシュ値を計算し、それを I C 部の内部不揮発性メモリに格納し、ハッシュ値に対して電子署名を生成する。データのセキュア領域からの読み出し時（復号化後）には、再度ハッシュ値を計算し、書き込み時に I C 部の内部不揮発性メモリに格納したハッシュ値と比較することでデータの欠損、改ざんなどを検知する。

こうした機能を搭載することで、このセキュアメモリカードは、決済する際に利用することもできるし、何らかのデータに電子署名を付与する際にも利用することができる。

また、このセキュアメモリカードを用いるR/W装置として、デジタルコンテンツ配信サービス用アプリケーションを搭載し、決済機能と、コンテンツのダウンロード及びメモリカードへの格納機能とを持つ場合について説明したが、セキュアメモリカードを活用する上で、R/W装置には次の機能を持つことが求められる。

- ・セキュアメモリカードの通常領域を読み書きするためのコマンドを生成することができる。
- ・セキュアメモリカードのIC部に処理を要求するためのICコマンドを生成することができる。
- ・IC部アプリケーション（IC認証部）と認証を行うための認証鍵を取得して、それを用いて認証に必要なデータ（IC部アプリケーションから提供された乱数に対して暗号または署名を施したデータ）を生成することができる。

また、セキュアメモリカードが通常領域として、非認証領域及び認証領域を有する場合には、これに加えて、

- ・認証領域を読み書きするためのコマンドを生成することができる。
- ・セキュアメモリカードの制御認証部と認証を行うための認証鍵を取得して、それを用いて認証に必要なデータを生成することができる。

ことが求められる。

なお、認証鍵の取得は、R/W装置（電子機器）が認証鍵をROMなどで保持している場合には、そこから入手する。また、電子機器が認証鍵を保持していない場合には、外部の機器（サーバ、リムーバブルメディア等）から受信する。

また、本発明のセキュアメモリカード10が有する大容量不揮発性メモリ50を、他の記憶メディア、例えば、ハードディスク、光ディスク、光磁気ディスク等の不揮発メディアに置き換えて、本発明と同様、大容量・高セキュリティなメモリデバイスが実現されることは言うまでもない。

また、本発明のセキュアメモリカード 10 は、電子機器に対して着脱可能である必要は無く、例えば電子機器に ICチップを埋め込んだ一体型機器などのように、電子機器と固定的に接続されていても良い。また、カード／チップのような形状である必要もなく、ディスクやテープなどの形態であっても一向に構わない。

5 また、本発明の電子機器（60、61、69）は、固定設置端末、携帯端末、携帯電話など、メモリデバイスが接続できるものであればどのようなものでも一向に構わない。

つまり、本発明の実施形態で説明したもの以外でも、携帯電話に ICチップを埋め込んだもの、固定設置端末にハードディスクを装着したようなもの等、その  
10 用途に応じて様々な形態が考えられる。

本発明を詳細に、また、特定の実施態様を参照して説明したが、本発明の精神と範囲を逸脱することなく、様々な変更や修正を加えることができることは、当業者にとって明らかである。

15 本出願は、2002年12月16日出願の日本特許出願（特願2002-363597号）に基づくものであり、その内容は、ここに参照して取り込まれる。

#### ＜産業上の利用可能性＞

20 以上の説明から明らかなように、本発明のメモリデバイスは、セキュリティレベルが ICカードと同等であって、記憶容量が ICカードに比べて遥かに大きいメモリ領域を持つことができる。

また、このメモリデバイスは、複数のセキュリティレベルのメモリ領域を備えており、一つのデバイスでデジタルキャッシュや音楽配信等の多用なサービスに対応することができる。また、この複数のメモリ領域の大きさは、必要に応じて  
25 変更することができる。

また、本発明の電子機器（R／W装置）は、このメモリデバイスを活用して、多様なサービスの実現を図ることができる。

## 請求の範囲

1. 電子機器に固定的にまたは着脱可能に接続されるメモリデバイスであつて、

前記電子機器からアクセスすることが可能な通常領域と、前記電子機器から直接アクセスすることができないセキュア領域とを有する、非耐タンパー性の第1のメモリと、

前記電子機器から直接アクセスすることができない耐タンパー性の第2のメモリと、

前記第2のメモリへのアクセスを管理するセキュア制御部と、  
を備えており、

前記電子機器から前記第1のメモリのセキュア領域へのアクセスは、前記セキュア制御部を介してのみ可能であること、

を特徴とするメモリデバイス。

2. 請求項1に記載のメモリデバイスであつて、

前記セキュア制御部は、前記セキュア制御部が認証した電子機器のコマンドを受けて前記セキュア領域または第2のメモリにアクセスし、データの書き込みまたは読み出しを行うこと、

を特徴とするメモリデバイス。

3. 請求項1または請求項2に記載のメモリデバイスであつて、

前記第2のメモリには、暗号鍵が格納されており、

前記セキュア制御部は、前記セキュア領域に書き込むデータを前記暗号鍵を用いて暗号化して書き込み、且つ、前記セキュア領域から読み出したデータを前記暗号鍵を用いて復号化すること、

を特徴とするメモリデバイス。

4 請求項1から請求項3のいずれかに記載のメモリデバイスであつて、

前記セキュア制御部は、前記セキュア領域に書き込むデータのハッシュ値を計算して、前記ハッシュ値を前記第2のメモリに格納し、前記セキュア領域から読み出したデータのハッシュ値を計算して、前記第2のメモリに格納したハッシュ値と照合すること、  
を特徴とするメモリデバイス。

5 請求項1に記載のメモリデバイスであって、

前記第1のメモリの通常領域が、メモリデバイスを制御する全体制御部によって認証された電子機器のみがアクセスできる認証領域と、認証を受けない電子機器でもアクセスできる非認証領域とを含むこと、  
を特徴とするメモリデバイス。

6 請求項1から請求項5のいずれかに記載のメモリデバイスであって、

前記通常領域と前記セキュア領域との境界を示す境界アドレス情報と、前記通常領域及びセキュア領域の各々における論理アドレスと物理アドレスとの関係を記述した論理-物理アドレス変換テーブルとが、前記第1のメモリのアドレス情報として管理されていること、  
を特徴とするメモリデバイス。

7. 請求項6に記載のメモリデバイスであって、

前記第1のメモリのアドレス情報に、前記認証領域と前記非認証領域との境界を示す境界アドレス情報と、前記認証領域及び非認証領域の各々における論理-物理アドレス変換テーブルとが含まれていること、  
を特徴とするメモリデバイス。

8. 請求項6または請求項7に記載のメモリデバイスであって、

前記境界アドレス情報及び論理-物理アドレス変換テーブルが、前記第1のメモリのアドレス情報管理領域に記録されていること、  
を特徴とするメモリデバイス。

9 請求項 6 に記載のメモリデバイスであって、  
前記境界アドレス情報で表された前記通常領域と前記セキュア領域との境界が、  
前記セキュア制御部の認証を受けた電子機器のコマンドで変更されること、  
を特徴とするメモリデバイス。

10 請求項 7 に記載のメモリデバイスであって、  
前記境界アドレス情報で表された前記認証領域と前記非認証領域との境界が、  
前記全体制御部の認証を受けた電子機器のコマンドで変更されること、  
を特徴とするメモリデバイス。

11 請求項 10 に記載のメモリデバイスであって、  
前記認証領域と前記非認証領域との境界の境界アドレス情報が、実境界アドレスと、セキュア領域を除いて設定したみなし境界アドレスとから成り、  
前記全体制御部の認証を受けた電子機器のコマンドによって指定された前記みなし境界アドレスに基づいて、前記実境界アドレスが変更されること、  
を特徴とするメモリデバイス。

12 メモリ領域として第 1 領域、第 2 領域、及び第 3 領域を有するメモリデバイスに対して、アクセスを行う電子機器であって、  
前記電子機器は、メモリデバイスへのアクセス要求を受けると、  
メモリデバイスの非耐タンパー性のメモリ領域である前記第 1 領域に、メモリデバイスへのアクセスを制御するメモリデバイスの全体制御部を介してアクセスし、  
前記全体制御部、並びに、第 2 領域及び第 3 領域へのアクセスを制御するメモリデバイスのセキュア制御部の認証を受けた後、第 1 領域以外の非耐タンパー性のメモリ領域である前記第 2 領域には、前記セキュア制御部を介してアクセスし、

前記セキュア制御部との認証を経た後、メモリデバイスの耐タンパー性のメモリ領域である前記第3領域には、前記全体制御部及び前記セキュア制御部を介してアクセスする、  
ことを特徴とする電子機器。

1 3. 請求項1 2に記載の電子機器であって、

第1領域に対するデータの書き込みまたは読み出しのコマンドを生成する第1のコマンド生成手段と、

セキュア制御部に処理を要求するコマンドを生成する第2のコマンド生成手段と、

前記セキュア制御部との認証に用いる認証鍵を取得し、前記セキュア制御部との認証処理を行う第1の認証処理手段と、

を備える電子機器。

1 4. 請求項1 2または請求項1 3に記載の電子機器であって、

第1領域の一部の領域である非認証領域には、全体制御部との認証を経ることなくアクセスを行い、非認証領域以外で、第1領域の一部または全部の領域である認証領域には、全体制御部との認証を経た後にアクセスを行う、

ことを特徴とする電子機器。

1 5. 請求項1 4に記載の電子機器であって、

認証領域に対するデータの書き込みまたは読み出しのコマンドを生成する第3のコマンド生成手段と、

全体制御部との認証に用いる認証鍵を取得し、前記全体制御部との認証処理を行う第2の認証処理手段と、

を備える電子機器。

図 1

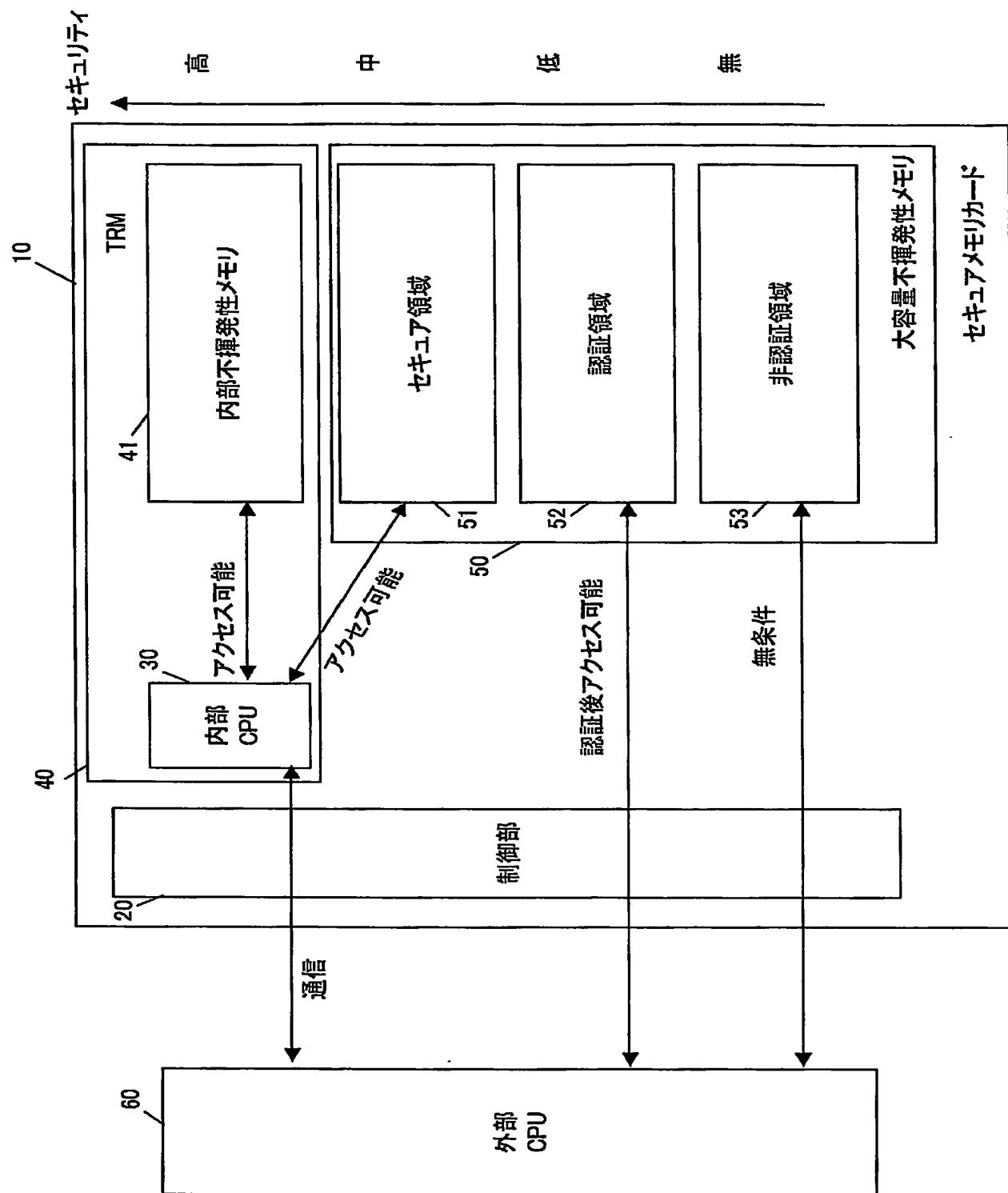
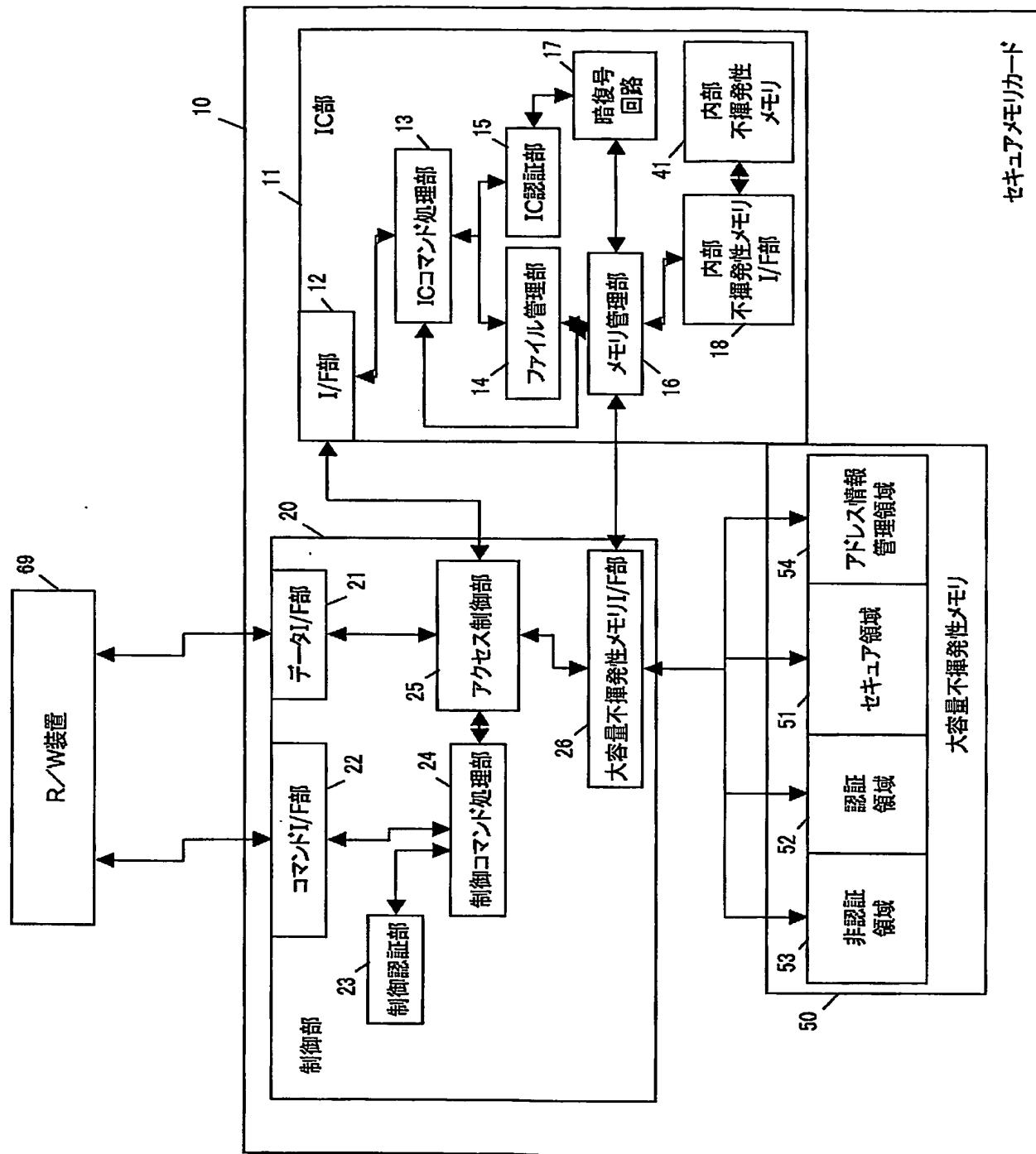


図 2



四 3

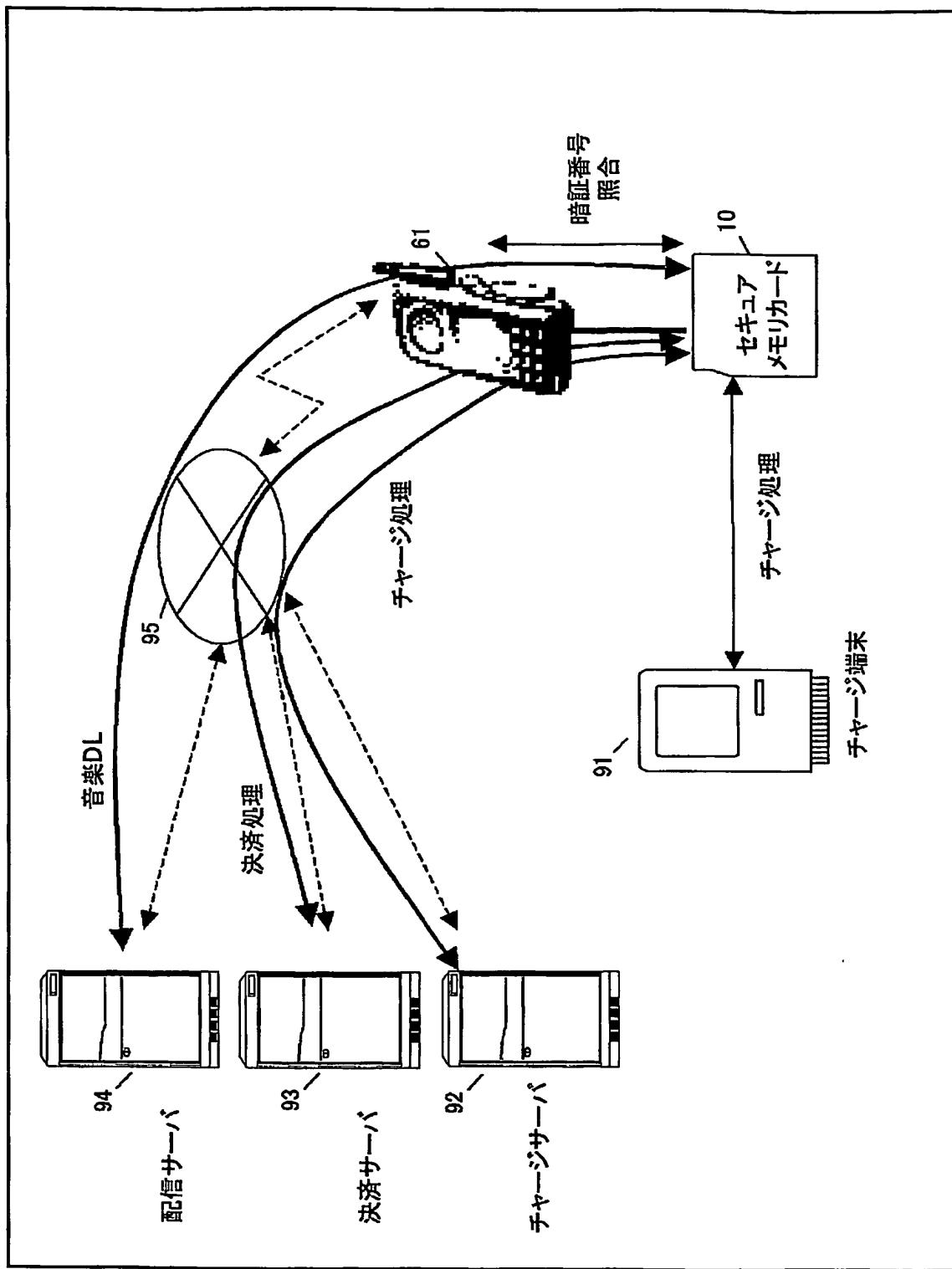


図 4

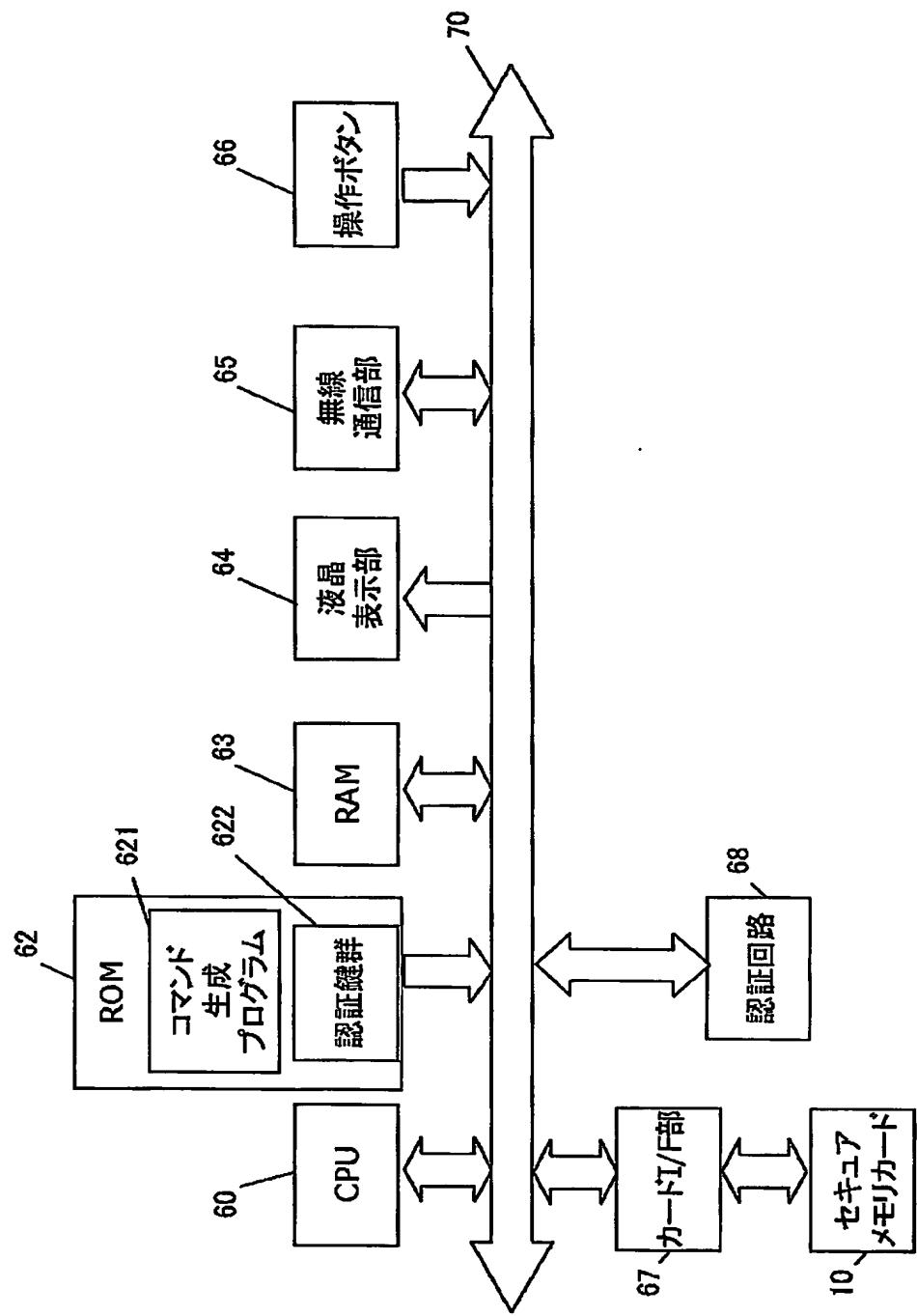


図 5

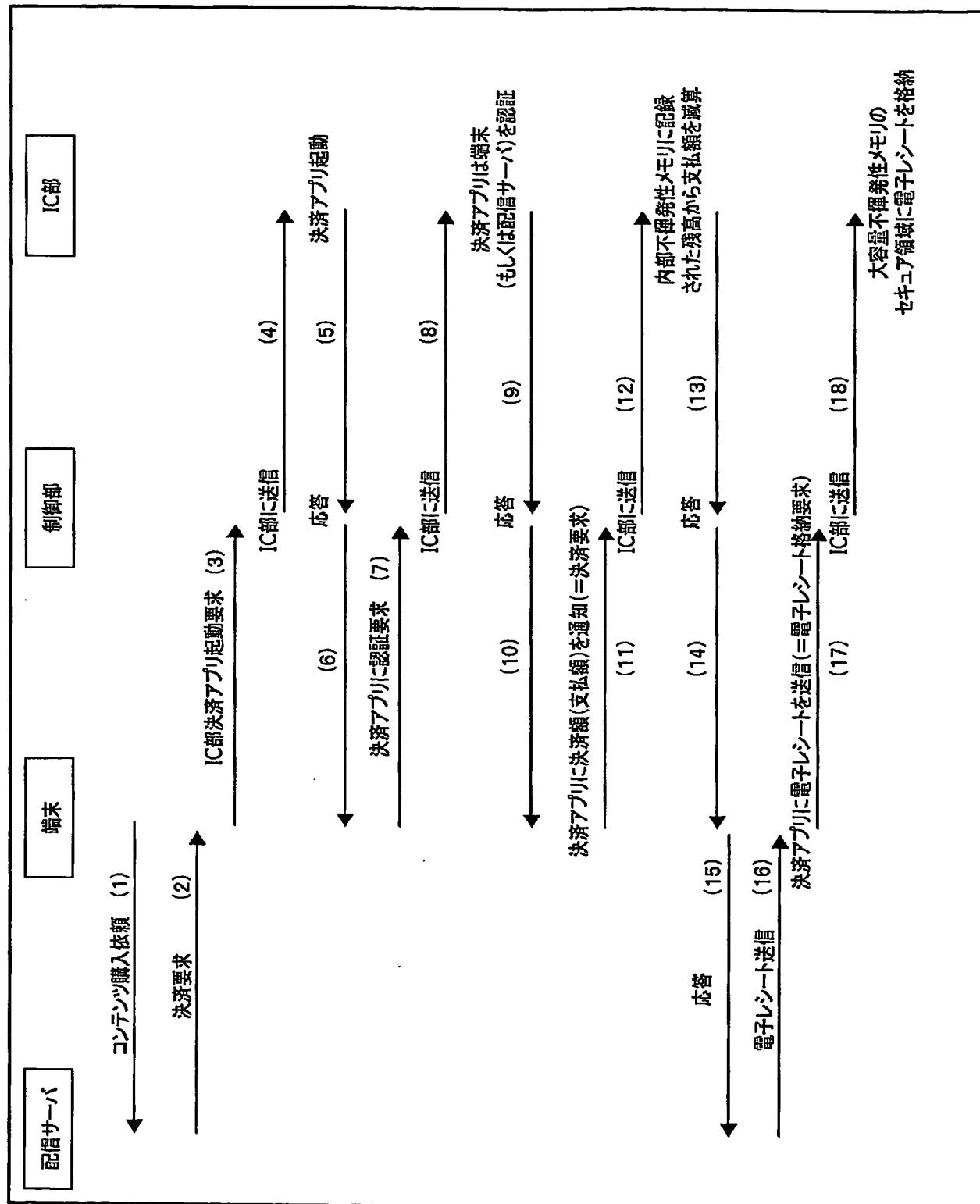


図 6

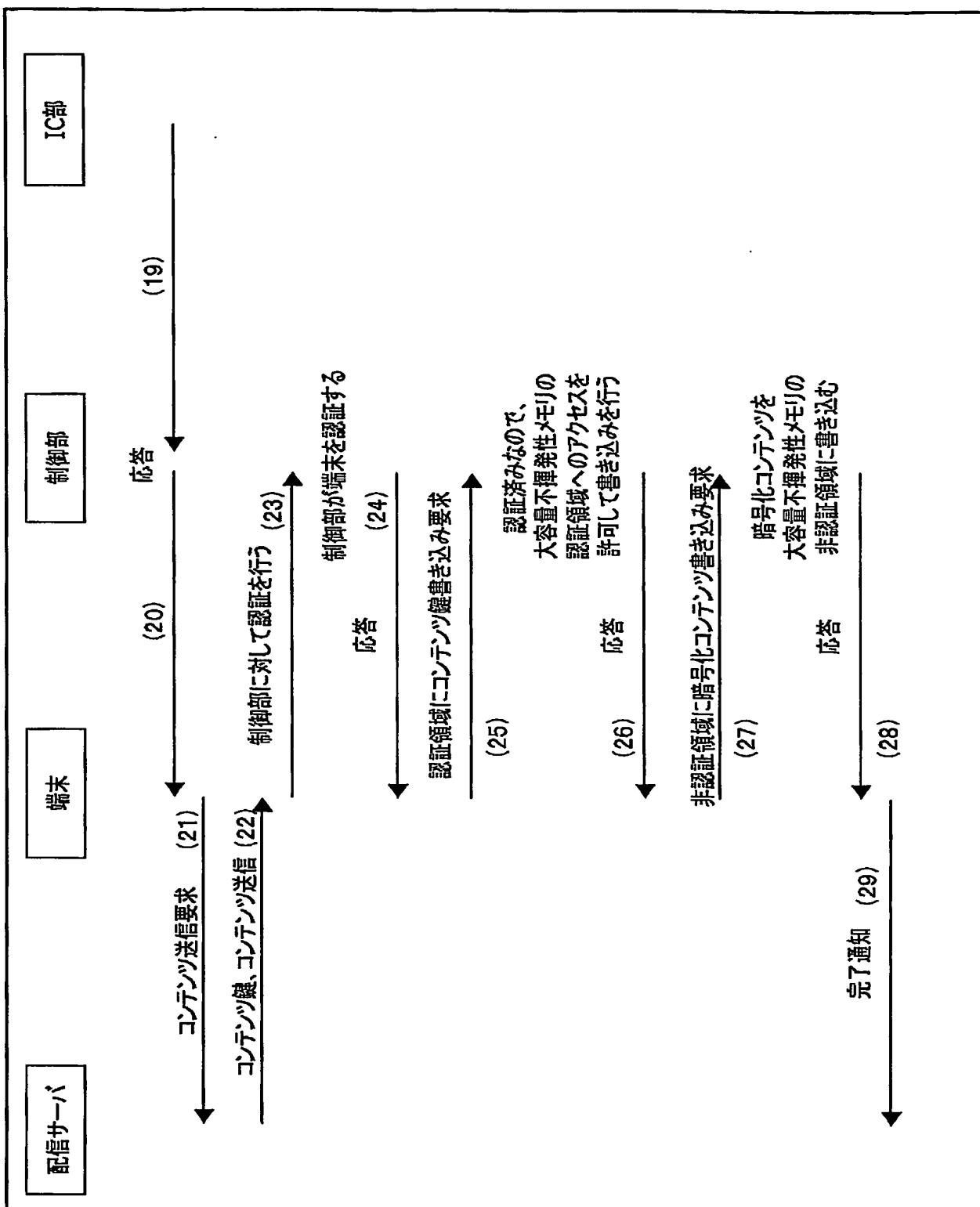


図 7

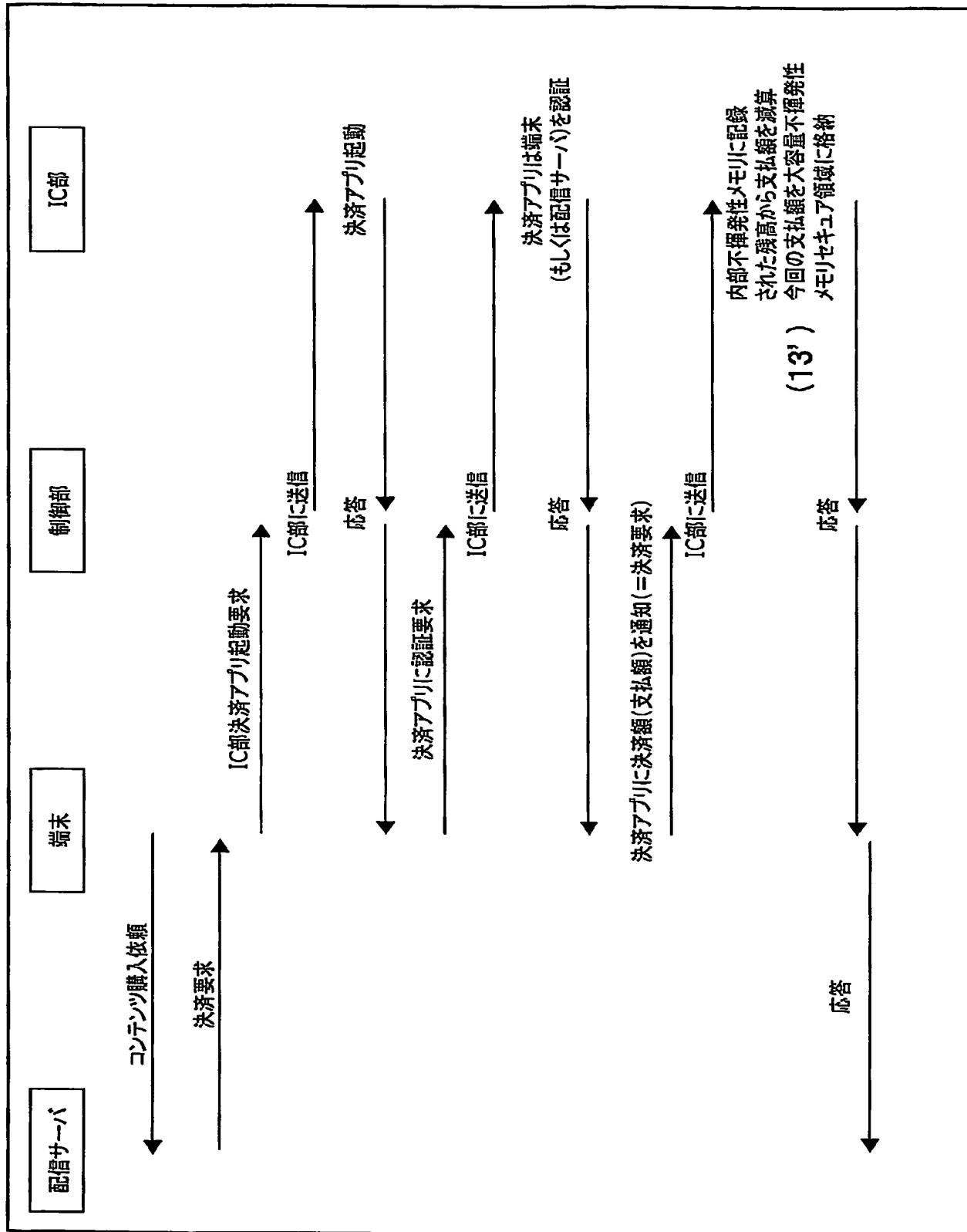
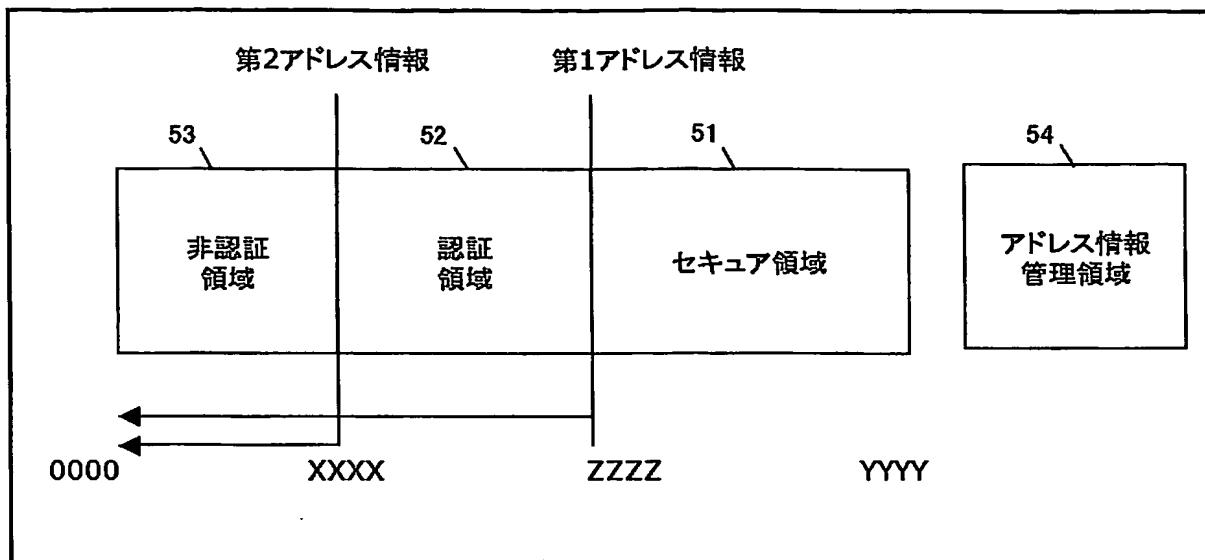


図 8



四 9

図 10

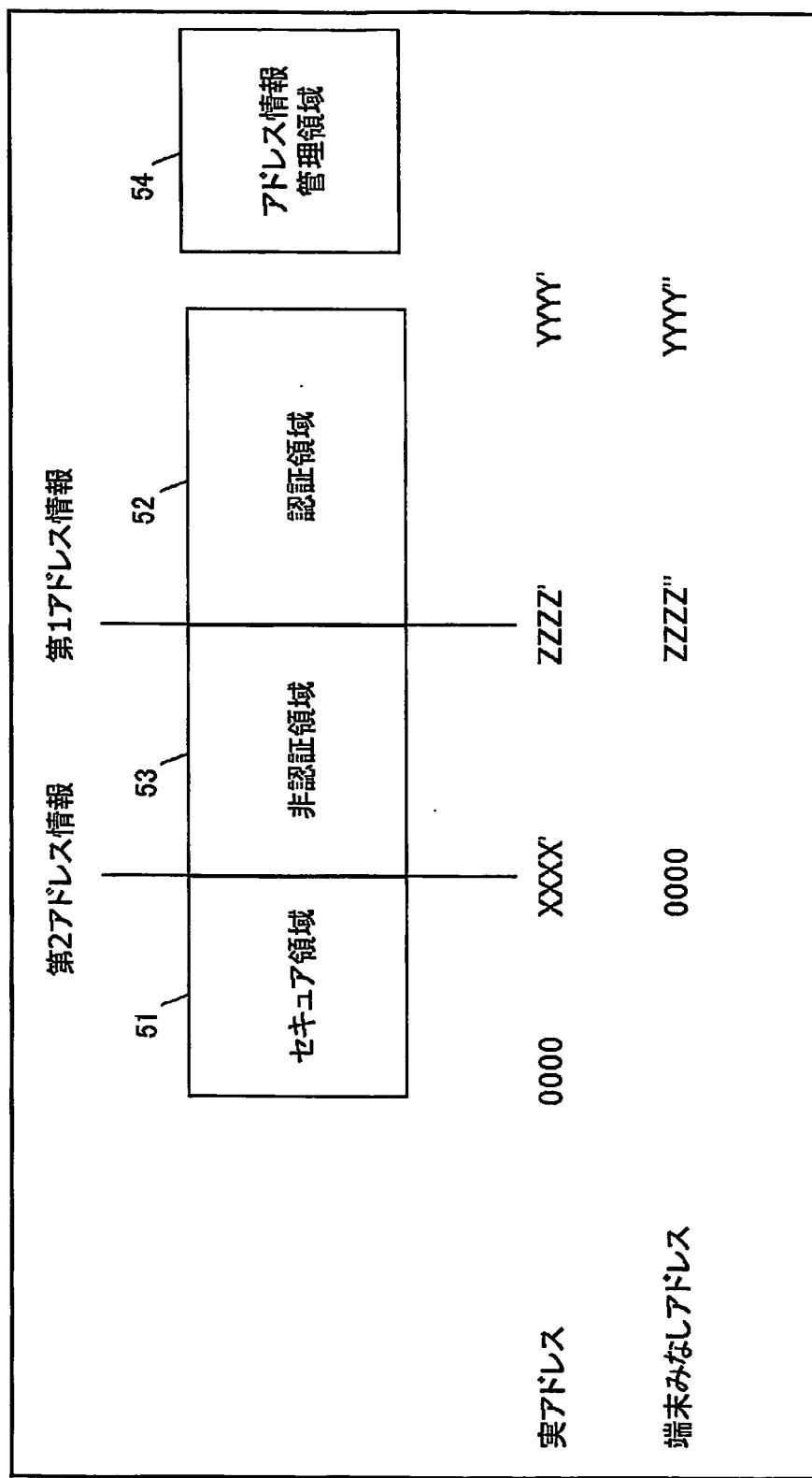
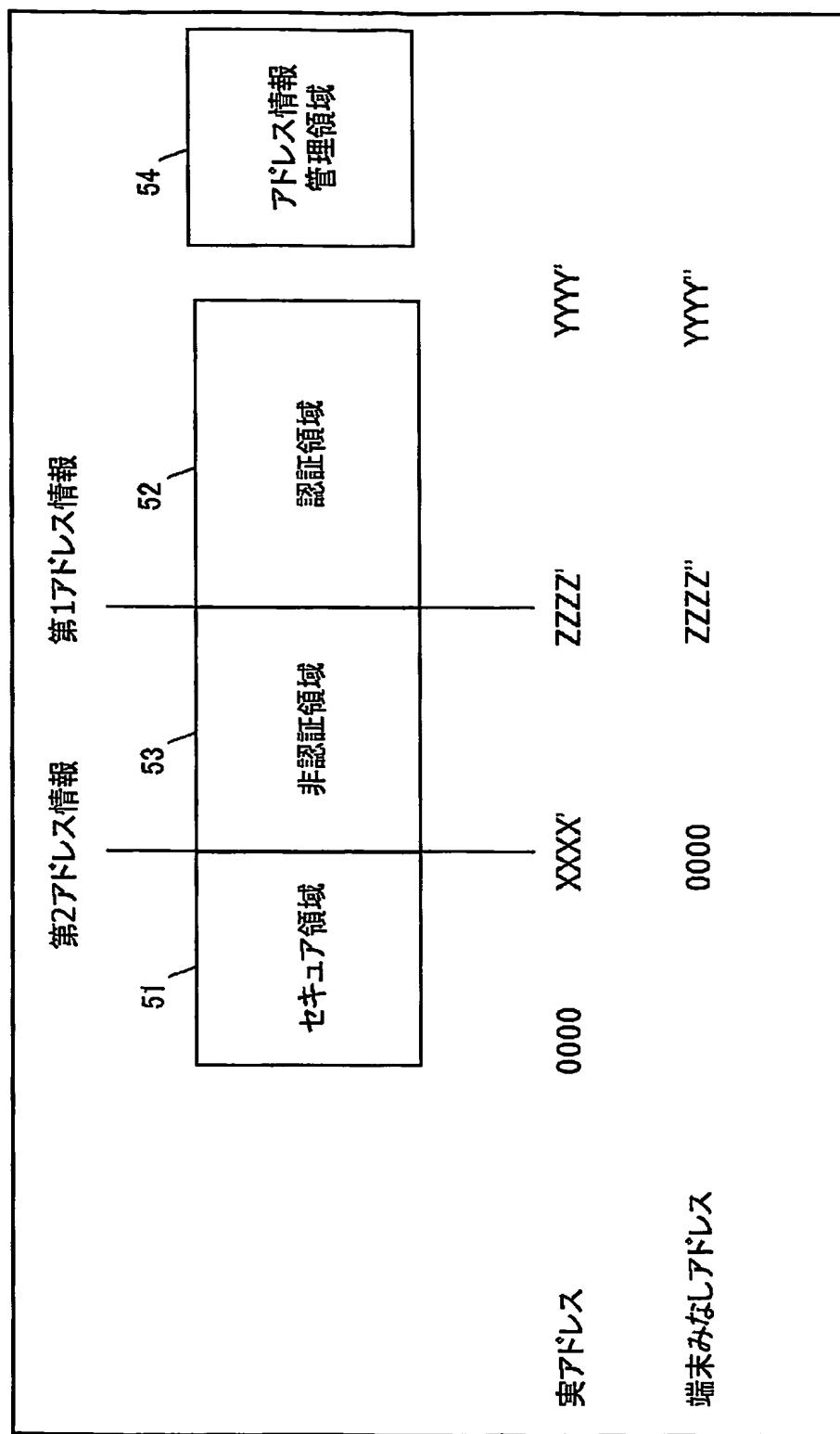


図 1 1



## 図12

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/16000

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F12/14, G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F12/14, G06K19/073

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2002-229861 A (Hitachi, Ltd.), 16 August, 2002 (16.08.02), Full text; all drawings & US 2002/169960 A1 & KR 2002065855 A	1-4, 12-15 5-11
Y	JP 2001-14441 A (Matsushita Electric Industrial Co., Ltd.), 19 January, 2001 (19.01.01), Full text; all drawings & EP 1050887 A1 & EP 1050887 B1 & JP 3389186 B2 & JP 2003-233795 A & WO 2000/65602 A1 & AU 200036750 A & CN 1316087 A & KR 2001083073 A & BR 200007581 A	5-11

 Further documents are listed in the continuation of Box C. See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search  
10 March, 2004 (10.03.04)Date of mailing of the international search report  
23 March, 2004 (23.03.04)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（IPC））  
Int.C1.7 G06F 12/14, G06K 19/073

## B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））  
Int.C1.7 G06F 12/14, G06K 19/073

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2002-229861 A(株式会社日立製作所) 2002.08.16, 全文, 全図	1-4, 12-15
Y	& US 2002/169960 A1 & KR 2002065855 A	5-11
Y	JP 2001-14441 A(松下電器産業株式会社) 2001.01.19, 全文, 全図 & EP 1050887 A1 & EP 1050887 B1 & JP 3389186 B2 & JP 2003-233795 A & WO 2000/65602 A1 & AU 200036750 A & CN 1316087 A & KR 2001083073 A & BR 200007581 A	5-11

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

- 「A」特に関連のある文献ではなく、一般的技術水準を示すもの
- 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
- 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
- 「O」口頭による開示、使用、展示等に言及する文献
- 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

- 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
- 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
- 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
- 「&」同一パテントファミリー文献

国際調査を完了した日

10.03.2004

国際調査報告の発送日

23.3.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

桜井 茂行

5N 2945

電話番号 03-3581-1101 内線 3545